UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,911	11/16/2001	Mark Crosbie	10012198	7932

7590 08/09/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
08/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/987,911	CROSBIE ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 13-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 13-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on May 21, 2007. Claims 1-6, 13-20 were pending. Claims 21-24 have been added per the received amendment.

2. Claims 1-6, and 13-24 are currently pending consideration.

Response to Arguments

2. Applicant's arguments with respect to claims 1-6, and 13-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, and 13-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moran (U.S. Patent 6,647,400) in view of Flint et al. (U.S. Patent 6,453,419).

Regarding claim 1, Moran discloses:

reading an event representing at least one system call (column 7 line 65 – column 8 line 23, column 13 lines 26-42);

routing the event to a template, the event comprising multiple parameters and the template comprising a sequence of connected logic nodes comprising at least one input node, at least on filter node, and at least one output node (column 7 line 65 – column 8 line 23, column 8 lines 12-35, column 14 lines 13-31);

filtering the event, based on the sequence of logic nodes of the template, as a possible intrusion based on the multiple parameters and either dropping the event or outputting the event, the filtering comprising: (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59):

determining a filename based on the event (column 11 lines 29-32, column 31 lines 31-35);

outputting the event for each event indicating modification of a critical file based upon the determined filename (column 32 lines 48-60); and

creating an intrusion alert for each event output from said filtering (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-60).

Moran does not explicitly disclose that the even representing a system call is a kernel audit record read from an intrusion detection data source (IDDS). However, Flint discloses a system that has the kernel log messages to the audit subsystem in order to form filters (Flint: column 11, lines 19-45). Moran discloses that the inventive system scans log files looking for evidence (events) so that an alert can be issued (Moran:

column 11, lines 45-55). Moran and Flint are analogous arts as both of pertain to implementing a security policy. Since Moran discloses searching log files for inconsistencies, and the security filters of Flint depend on the kernel audit logs, it would have been an obvious variation to use the system of Moran to search the kernel audit logs as well. Therefore, it would have been obvious to one of ordinary skill in the art to scan kernel audit logs for inconsistencies since the kernel audit logs are used to "implement filters" (Flint: column 11, lines 43-46).

7. With respect to claim 14, Moran discloses a system for detecting critical file changes, comprising:

a processor (column 5 lines 26-42);

a memory storing instructions which, when executed by the processor, cause the processor to:

route events to a template (column 7 line 65 – column 8 line 23, column 14 lines 13-31);

wherein the event comprises one or more parameters (column 11 lines 15-65, column 32 lines 48-59); and

the template comprises a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node (column 7 line 65 – column 8 line 23, column 8 lines 12-35, column 14 lines 13-31);

filter the event as either a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59); and

create an intrusion alert if an event is output from the filter (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59).

Moran does not explicitly disclose that the even representing a system call is a kernel audit record read from an intrusion detection data source (IDDS). However, Flint discloses a system that has the kernel log messages to the audit subsystem in order to form filters (Flint: column 11, lines 19-45). Moran discloses that the inventive system scans log files looking for evidence (events) so that an alert can be issued (Moran: column 11, lines 45-55). Moran and Flint are analogous arts as both of pertain to implementing a security policy. Since Moran discloses searching log files for inconsistencies, and the security filters of Flint depend on the kernel audit logs, it would have been an obvious variation to use the system of Moran to search the kernel audit logs as well. Therefore, it would have been obvious to one of ordinary skill in the art to scan kernel audit logs for inconsistencies since the kernel audit logs are used to "implement filters" (Flint: column 11, lines 43-46).

8. With respect to claims 2 and 15, Moran discloses a method, wherein said filtering further comprises providing the event to the determining a file name for each event

comprising a parameter indicating modification of a permission bit on a file or directory (column 9 lines 33-47).

9. With respect to claims 3 and 16, Moran discloses a method, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating opening a file for truncation (column 11 lines 15-48, column 31 lines 31-56).

10. With respect to claims 4 and 17 Moran discloses a method, wherein said filtering comprises providing the event to the determining a filename for each event comprising a parameter indicating modification of the ownership or group ownership of a file (column 9 lines 33-47, column 31 lines 30-57).

11. With respect to claims 5 and 18, Moran discloses a method, further comprising outputting an alert message for each renamed file including the filename of the file and the new filename of the renamed file (column 9 lines 33-47, column 30 lines 7-13).

12. With respect to claim 6 and 19, Moran discloses a method, comprising configuring a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable (column 32 lines 60-67).

13. With respect to claim 13, Moran discloses a computer-readable medium storing instructions which, when executed by a processor, cause the processor to implement the method steps of claim 1 (column 5 lines 26-42, column 7 line 65 – column 8 line 23, column 11 lines 15-65, column 13 lines 26-42, column 32 lines 48-59).

14. With respect to claim 20, Moran discloses a system, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a filename based on the event and output the event for each event indicating modification of a critical file based upon the determined filename column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-60).

15. With respect to claim 21, Moran discloses the method of claim 1, wherein said filtering further comprises determining a subdirectory of a directory based on the event and outputting the event for each event indicating a modification to the determined subdirectory (column 9 lines 33-47).

16. With respect to claim 22, Moran discloses the system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a subdirectory of a directory based on the event and output the event for each event indicating modification to a predetermined subdirectory of a directory (column 9 lines 33-47).

17. With respect to claim 23, Moran discloses the method of claim 1, wherein said reading an event comprises reading an event from an event-driven correlation service of the IDDS (column 13, lines 35-42).

18. With respect to claim 24, Moran discloses the system of claim 14, wherein the instructions causing the processor to read an event comprise instructions causing the processor to read an event from an event-driven correlation service of the IDDS (column 9 lines 33-47).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA. 8/5/07)

KA
08/05/2007

SYED A. ZIA 8/15/2007
PRIMARY EXAMINER